# 区块链技术在网络舆情风险管理体系的应用研究

■ 郭苏琳　黄微　李吉
吉林大学管理学院　长春 130022

摘　要：[目的/意义] 挖掘弹性管理和区块链理论在网络舆情风险管理体系建设的应用价值，克服传统管理体系的技术弊端，突破现有网络舆情风险管理的难点和痛点，提高网络舆情风险管理效率。[方法/过程] 基于网络舆情风险管理、弹性管理理论，确立网络舆情弹性风险管理的理论框架，进而应用区块链技术提出网络舆情风险管理系统体系，并对网络舆情风险识别和感知智慧分类账本、风险关联树以及智能合约进行详尽阐述。[结果/结论] 构建的舆情风险管理系统、区块链数据保障系统体系，及应用区块链技术的网络舆情风险识别和感知智慧分类账本、风险关联树、智能合约，使得舆情风险管理数据更安全、数据可追溯、组织弹性适应性更强，能有效指引有关系统开发，并增强网络舆情风险管理可控性、提高网络舆情风险管理效率。

关键词：区块链　网络舆情　风险管理
分类号：TP393
DOI：10.13266/j.issn.0252－3116.2020.09.003



## 1　引言

自 1991 年区块链技术被提出以来，区块链就以其独特的魅力在众多领域扎根发芽。从受众熟知的比特币所代表的区块链 1.0，到基于智能合约的以太坊区块链 2.0，再到如今更具产业应用价值的“区块链 ×”应用，区块链的应用场景逐步扩展并给各行各业带来了颠覆性的改变以及更具突破性的创新空间[1]。区块链技术应用于网络舆情管理及舆情风险感知识别领域，可以重构舆情信息生态系统、提高舆情信息价值密度、杜绝虚假舆情信息发布、加强舆情用户隐私保护、为舆情风险识别和感知提供去伪存真的坚实数据基础[2]。然而，区块链技术在网络舆情管理领域的理论研究、应用实践和思想渗透等方面却较为滞后，特别是在网络舆情风险感知及识别领域更少有学者关注。同时，在融媒体环境下，舆情信息扩散速度更快、影响面更广、线上线下融合集聚破坏力更强，若舆情主题涉及到突发事件、社会敏感事件则更容易爆发大规模的群体性事件，甚至是危害和谐小康社会建设的危机事件。从而，给政府和监管部门有效应对舆情风险带来前所未有的压力和挑战。而在舆情风险管理的识别、分析、应对过程中，舆情风险感知基础上的准确识别更是有效应对舆情风险的基石。

因而，笔者基于现有区块链、网络舆情管理理论，针对网络舆情管理的难点和痛点，提出一种基于区块链技术的网络舆情风险管理体系，以解决以下 3 个方面的理论和实践问题：①如何基于风险管理和网络舆情管理理论，确立网络舆情风险感知及识别理论框架？解决舆情风险管理的系统弹性、舆情风险感知和识别精度提升、舆情风险分析准确性、舆情风险动态应对持续性、舆情风险关联大数据库建设、舆情风险控制窗口期的即时响应等关键问题。②如何基于区块链和网络舆情管理理论，构建网络舆情风险管理系统体系？解决舆情风险管理数据完整性、数据鉴别、独立第三方审查、管理审查和问责、数据更新和资源充足性等系统功能性问题，同时弥补传统系统存在的数据安全性低、数据真实性难以保障、数据易丢失损坏等缺陷。③怎样基于区块链理论，设计网络舆情风险管理智慧分类账本、风险关联树以及智能合约？解决舆情风险管理数据追溯和篡改、舆情风险分担机制数据支撑、舆情风险追踪、舆情风险管理绩效设计、重大舆情风险分析准确性、舆情风险预警水平提升、舆情应对自动化响应等关键问题。

作者简介：郭苏琳（ORCID：0000－0002－9941－4988），博士研究生，E-mail：148046941@qq.com；黄微（ORCID：0000－0003－0448－9563），教授，博士，博士生导师；李吉（ORCID：0000－0003－083－5733），博士研究生。
收稿日期：2019－09－20　修回日期：2020－01－18　本文起止页码：19－26　本文责任编辑：徐健

## 2 文献回顾

### 2.1 区块链技术研究现状

作为21世纪技术革命进步领域的区块链技术,其核心优势是去中心化,以及通过链式数据结构加密、时间戳、工作量证明和共识机制等手段,为传统中心化模式存在的信息安全、共信低效、交互成本高等问题提供了解决方案[3]。区块链架构没有中心服务器,一般来说包括分布式网络、底层数据、分布式账本、共识机制以及网络应用5个部分[4],所有节点都是无需信任的对等关系,数据库的建立不可变更、伪造和撤销,所有数据都可以追溯[5]。以区块形式存储的底层数据基于共识机制进行验证[6],共识机制可以创建新的区块,允许代理通过时间戳按照交易顺序记录系统状态。在任何场景中,创建区块需要成本的特性在一定程度上遏制了垃圾信息的生产,大幅提升了系统安全,破坏了虚假信息传播的土壤,缓和了中介机构矛盾并形成共赢。

随着区块链应用场景的逐步深入,区块链技术的研究也取得了长足发展。H. W. Kim 等[7]采用区块链技术提升移动存储设备计算能力和存储容量,在移动设备资源认证基础上,搭建移动设备资源信息链。M. E. Greiner[8]介绍了无信任系统的概念,并提出对等系统中如何解决信任问题的建议。通过可信任的中间人建立代价高昂的信任机制这种传统做法,将被基于分散算法和智能合约的密码协议所取代。E. Dmitry 等[9]指出区块链技术通过公钥加密和对等网络来解决信任问题将会颠覆很多行业。R. Beck 等[10]将这一概念应用于基于区块链视角的商业系统,并开发了一个交易系统概念原型,该交易系统基于共识的交易规则无需相互信任的自主运行。然而,无需信任的概念目前还存有争议,有学者认为信任不会被取代,而是从中央机构转移,或者市场信任需要建立在对算法权威的认可基础上,这最终控制了代理的相互作用[11]。除此之外,了解分布式账本、分散共识系统的技术协议和实现,以及分散应用仍然很复杂,研究人员和从业者应努力挖掘并充分发挥区块链的全部潜能。

### 2.2 网络舆情风险管理研究现状

在风险管理中,风险识别建立在风险感知基础上[12],网络舆情风险感知则是指人们从决策支持的角度对网络舆情可能给网民及社会带来的各种风险的分析和判断。舆情风险识别则是在舆情风险感知基础上,运用各种方法,系统、连续地对可能产生一定破坏力的舆情事件传播特征和规律进行归纳总结,发现影响舆情走势的关键因素,挖掘关键时间节点和发现意见领袖,从而为后续舆情风险应对提供坚实的支撑。

目前,学者主要从普通网民视角,分析影响个体舆情事件风险感知因素。例如,王炼和贾建民[13]将网络搜索作为网民风险感知水平的指标,利用关键词分析法,从空间分布和时间演变两个维度分析了网民风险感知的动态特征。A. Sugimoto 等[14]以福岛核泄露事件为例,在大量研讨会质性材料分析、问卷调查基础上,建立多元回归模型,并展开实证研究,研究结果揭示了舆情传播媒介和网民风险感知之间的潜在联系;在舆情风险评价方面,张玉亮[15]在突发事件网络舆情风险分析基础上,构建了3个层次的突发事件网络舆情风险评价指标体系,采用层次分析法展开实证研究。曾润喜等[16]提出应从政治、经济、文化、社会、生态5个方面对网络社会安全风险进行评价;在舆情风险综合识别方面,众多学者倡导管理学、情报学、生命科学等多学科交叉研究[17],王文艳等[18]以"3.1昆明暴恐事件"为例,从实践操作层面指出,舆情风险管理过程中的群体极化倾向、媒介舆情引导力度、政府公信力水平是识别舆情风险的要素。陈培友[19]以"重庆公交坠江事件"为例,采用灰色模糊评价方法,构建了社交网络舆情风险预警模型。L. Yu 等[20]从网民、舆论领袖、政府和大众媒体4个舆情信息主体出发,建立了舆情风险多主体仿真模型,并指出舆论传播速度、范围、信息披露程度等影响了舆情风险识别及处理效果。曾润喜[21]从非传统安全视角入手,从社会和技术环境两方面提出了网络舆情治理的新路径。

### 2.3 区块链技术在网络舆情信息管理领域研究现状

如前文所述,目前少有学者基于区块链理论展开网络舆情管理系统的研究,而对于网络舆情管理中的舆情风险感知及识别问题进行深入研究的文献则更少。尽管如此,国内外学者普遍认为,将区块链技术应用于信息管理及网络舆情管理领域,能够杜绝虚假信息的传播、提高信息价值密度、建立信息生产和消费者之间的互信、实现信息的回溯与追溯,从而重构网络信息生态环境,提高网络舆情管理效率、加大信息安全和隐私保护力度。M. Arquam[22]基于区块链技术构建了一个安全可信的网络信息传播框架,通过组合信息块创建链,网络中每个节点根据其可靠性将信息传播到其对等节点,节点的可信度将根据各自的信息而变化。信息生产者和信息消费者基于两种方式建立信任:①对等级别用户共享信息的本地信任,即信誉等级相同的用户在本地可以建立信息交互的信任;②网络中

每个舆情用户基于本模型的可信度检查结果建立全局信任。最后,笔者基于 Facebook 数据集对所构建的网络信息传播框架进行了分析,并达到了 83% 的准确率,验证了所构建框架的有效性。S. Ma 等[23]认为信息管理过程中要注重风险和信息系统控制,主要包括信息风险管理以及识别风险的方法和过程,需要对网络事件造成社会影响的可能性和严重程度进行评估,进而确定应对策略。因而,为了更好地达到信息回溯、可追溯、不可逆和可信性的要求,文章提出了一种基于区块链的信息风险及信息系统控制框架,基于默克尔(Merkle)树,设计了风险关联树,将风险项目分类帐本、风险分析分类帐本和风险应对帐本相结合,形成拟议的智能合约,用于信息风险识别、分析、应对、监控、引导和报告过程,并开发了系统原型。H. D. Huang 等[24]指出,虽然美国、韩国和中国在内的许多国家对数字虚拟货币发出警告并制定了相应的法规。但是,区块链虚拟货币背后的风险和欺诈问题不容忽视,以太坊智能合约的安全性并没有得到足够的重视。因而,研究团队提出了一种对以太坊社区评论进行情绪分析的机器学习方法,构建了 lstm + cnn 模型,基于社交网络收集的用户加密货币评论,对网民的情感进行分析和预测,并达到到 0.80 以上的情感分析准确率。

现有国内相关研究主要集中在区块链技术在网络舆情领域的应用意义及现实性探讨方面。赵丹等[25]以 Steemit 平台舆情信息为例,采用社会网络分析方法,对区块链舆情信息传播的特征和规律展开研究,并得出区块链环境下的网络舆情传播生态更为和谐的研究结论;宾晟等[26]在赵丹的相关研究基础上,基于传染病理论和博弈理论,构建了区块链环境下网络舆情传播 SEIR 模型,以 Steemit 数据为例进行了仿真研究,分析说明了区块链舆情网络中激励机制、收益和风险机制对舆情信息传播的影响;黄心豪和赵博[27]基于区块链技术展开了网络舆论优化研究,指出区块链技术可以在网络舆情信源追溯、舆情熔断机制、情绪预警机制建设方面进行有效应用;陈鹤杰和闫强[28]认为,出版社应该利用先进的网络工具和技术,对舆情事件进行重点关注,并进而以区块链热点事件为实证数据分析了其与出版社选题策划及图书销售的关联,反映了网络舆情和区块链技术在出版发行领域的应用价值;丁晓蔚和高淑萍[29]对虚拟货币舆情带来的金融风险展开了研究,研究发现区块链技术支撑下的虚拟货币舆情异常活跃,因而要加强金融监管和舆论引导,避免规避舆情风险和金融风险的同时矫枉过正而扼杀区块链金融创新;李泰安[30]对区块链技术给网络舆论环境带来的积极作用予以充分肯定,并认为区块链技术在网络舆情管理领域的应用,可以在版权保护、虚假新闻打击、个人隐私保护、信息脱敏等方面形成合力,从而凸显优质舆情信息内容,重构舆论环境。

## 3 网络舆情风险管理系统概念框架

为采用区块链技术,突破现有网络舆情风险管理的瓶颈,设计网络舆情弹性风险管理系统。本节在相关文献梳理基础上,按照传统风险管理理论到弹性风险管理理论,再延伸到网络舆情弹性风险管理理论框架设计的研究脉络展开。风险管理被视为一种持续性的管理行为,需要对风险事件影响进行准确预测,力图通过实施有效的风险管理和控制框架,采取风险应对措施,最大化地利用每一个可能的机会,从而减少风险管理失控可能对组织资产带来的损失和影响[31]。因而,基于传统风险管理理论,风险管理生命周期包括风险识别、风险分析、风险应对、风险控制和报告 4 个过程。

然而,传统风险管理理论虽然可应对定量化风险和可预测的威胁,但是在瞬息万变的网络环境下,网络舆情风险潜在的影响很大、不确定性更高,舆情管控主体不可能处理所有舆情风险,或者处理所有舆情风险的成本过高。从而,弹性风险管理理论所强调的"在高度不确定性环境预测并适应变化,从范围广泛的风险事件中吸收、恢复、抓住隐含在风险事件中的机会[32]。"对融媒体环境下的网络舆情风险感知和识别更具有理论适应性。即,发生网络舆情生态环境变化时,远离网络舆情均衡事件的高可变性和自适应性的"管理弹性",则可赋予网络舆情风险管理系统更好地承担和管理舆情风险的能力。进而,笔者结合传统风险管理理论和弹性风险管理理论提出了网络舆情风险管理系统概念框架,见图 1。

网络舆情风险对舆情管控目标实现也具有二重性影响,舆情风险管理信息系统的控制目标是发现潜在舆情风险、以适当方式承担舆情风险,确保将舆情风险降低到可接受的水平,从而在识别和分析舆情风险后,舆情管控主体可以弹性地选择适当舆情风险应对策略并制定实施行动计划。舆情风险报告必须定期监控并向舆情管控主题报告,监控舆情风险发展趋势、合法性和现存问题。

同时,内外部舆论环境的变化、技术进步以及其它舆情风险要素的变化和舆情生态的进化，也要求舆情

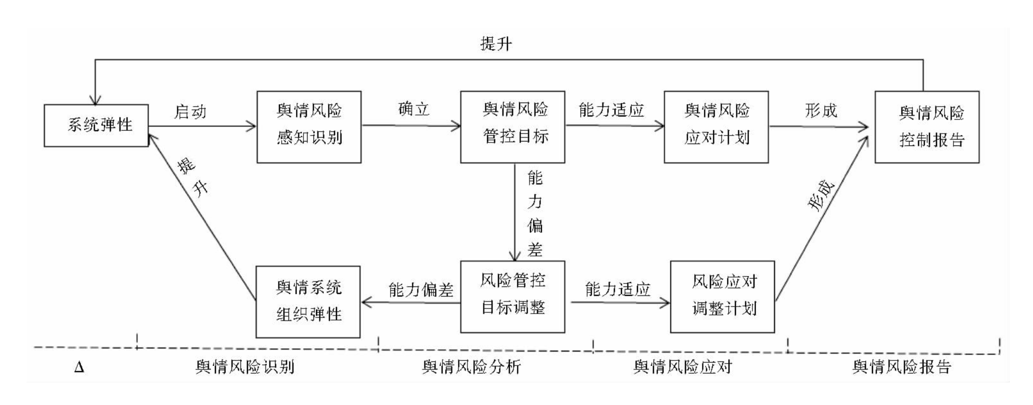



图 1 网络舆情风险管理系统概念框架

风险管控主体动态审视舆情风险管理工作，重新分析舆情风险甚至修订舆情风险应对计划。持续的舆情风险动态监控和控制、舆情风险关联数据库建设、对舆情风险数据的有效识别和舆情风险控制窗口期的即时应对响应等，都凸显了网络舆情弹性风险管理系统概念框架的先进性。

## 4 基于区块链的网络舆情风险管理系统设计

从非功能性需求层面审视现有可借鉴的各领域风险管理信息系统，可以发现大都存在以下 3 个方面的缺陷：①数据安全性低。即便是风险管理云平台，业务数据也一直受安全问题困扰，一旦数据库被黑客攻击，业务数据的泄露将带来不可估量的损失。②数据真实性难以保障。一方面电子数据容易被不留痕迹的篡改和删除，另一方面人工审核数据真实性耗费人力并且存在主观性。③数据易丢失损坏。风险相关利益者在对数据的存储和利用过程中，很容易造成数据丢失或损坏。而应用区块链技术的舆情风险管理系统的数据不可篡改、可追溯、存储去中心化，因而不存在数据库被黑客攻击问题，业务数据泄露可能性小，即便泄露也必然留下可追溯的痕迹，关键数据不再集中存储在个别机构，而是通过区块链 P2P 存储，降低了关键数据丢失损坏的可能性，极大提高了数据安全性。通过区块链智慧分类账和智能合约对电子数据和风险管理过程（交易）进行分类、比对和执行，提高了管理的效率，降低管理的主观性。从功能性需求层面，如前文所述，社交网络中虚假信息泛滥，相关机构对信息真实性鉴别所投入的时间和经济成本较高，亟待构建一个强大的、安全可信的舆情风险管理系统来解决上述问题。并且，舆情风险管理过程所涉及的舆情感知和识别、舆情风险分析、舆情风险应对、舆情风险报告环节，均要求所构建的风险管理系统达到功能全面、数据完整、可供独立第三方审查、可鉴别、符合政策法规、基于审查和问责的监控、数据及时更新、资源充足等要求。而区块链技术的应用，能很好地支撑舆情风险管理概念框架。基于以上分析，笔者提出了包含舆情风险管理系统、区块链数据保障系统 2 个交叉支撑子系统的网络舆情风险管理体系，见图 2。

### 4.1 舆情风险管理系统

舆情风险管理系统框架是一个遵循舆情演进生命周期的管理过程，系统弹性优化则是初始阶段，此阶段任务主要包括设置舆情风险偏好值，建立零风险项，灵活配置、整合内外资源要素，构建有效协调组织的运行机制。舆情风险管理系统框架则包括舆情风险感知和识别、舆情风险分析、舆情风险应对、舆情风险报告 4 个功能模块：①舆情风险感知和识别。舆情风险感知和识别模块基于舆情演化要素、风险感知识别模型和风险偏好各等级阈值感知、识别和记录舆情风险。舆情风险识别不仅包括识别舆情本身风险，还包括对组织本身、风险管理外部依赖条件和假设的风险识别，如舆情风险管理组织弹性、资源可用性或风险应对及时性。②舆情风险分析。在舆情风险登记簿上识别和记录舆情风险后，进入舆情风险等级分析阶段。对舆情潜伏、酝酿、爆发、消退、消亡时间节点进行分析，计算舆情线上或线下影响力，分析过程必须考虑舆情风险管理组织和舆情管理利益相关者的依赖关系，以及受影响的衍生舆情、相关舆情用户。有时甚至评估舆情风险管理组织公信力、舆情风险控制水平、群体性破坏事件可能性、舆情风险偏好和容忍之间的关系等。③舆情风险应对。舆情风险应对的关键是舆情风险管理组织弹性、感知识别及时性、等级评估准确性、应对计划科学性。这个阶段要求在恰当的时间节点提出有效、合理、科学的舆情风险应对决策，并提供详尽实施

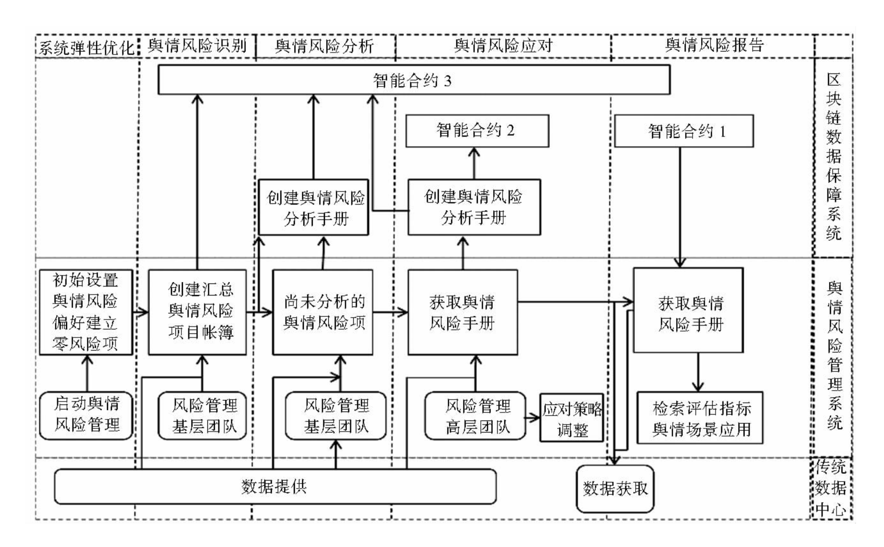


图 2　基于区块链的网络舆情风险管理体系结构

计划。④舆情风险报告。在精准的舆情风险感知、识别、监测、分析基础上，舆情风险管理组织已不在价值密度极低的繁杂数据中迷失，舆情风险控制已经被限定在一个条件合理、计划完备、环境可控的情境下，通过舆情风险控制绩效指标可以大大提高持续监控效率，并基于各绩效等级舆情风险报告建立舆情风险应对预案。

### 4.2　区块链数据保障系统

区块链数据保障系统采用区块链技术，构建包括风险识别、分析和应对计划的风险登记表，将风险识别、风险分析、风险应对和风险报告数据存储在区块链中，确保风险登记表数据可追溯并不可篡改，从而为建立舆情管理主体、网民和舆情风险管理硬件之间的风险分担机制提供数据支撑。基于关联树按照风险级别动态追踪不同舆情风险并建立舆情风险智能分类账。设计智能合约和舆情风险管理绩效表，提高重大舆情风险分析准确性，改善舆情风险预警水平，提升舆情应对自动化相应能力。

#### 4.2.1　基于区块链的舆情风险智慧分类账

在舆情风险智能合约中，舆情风险登记表形成于舆情风险识别过程，合约则根据舆情风险分析和舆情风险控制过程进行更新。舆情风险智能合约分为 3 类(见图 3)：①舆情风险汇总项目分类账，拥有完整的从舆情识别到舆情应对的风险账户；②舆情风险分析分类账，用于保存不同舆情风险事件账户的评估等级信息；③舆情风险应对分类帐，它保存唯一标识下的不同舆情风险事件账户舆情风险应对程序项目。

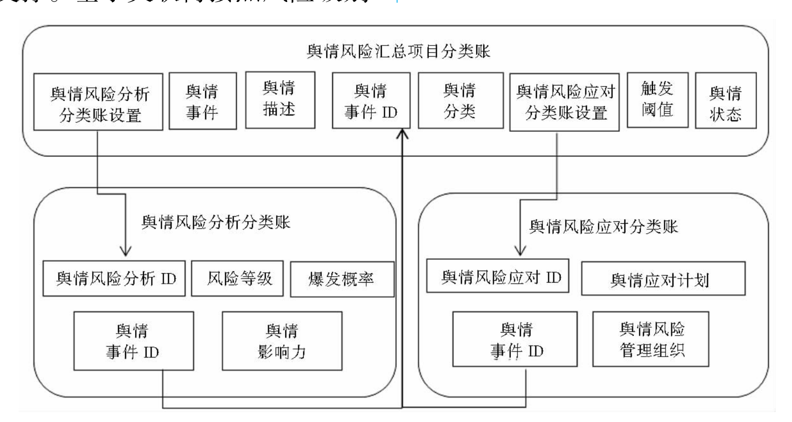


图 3　基于区块链的舆情风险智慧分类账

基于区块链的舆情风险智慧分类账具有以下 10 个关键属性：①舆情事件 ID。舆情风险管理者需要快速找到特定的舆情风险事件，因此使用唯一的标志 ID 来识别每个舆情事件。同时，对舆情事件的主题进行简单描述，对舆情应对成功或失败以及绩效进行标注。②舆情描述。补充舆情事件 ID 未涵盖或疏漏的信息，提供更详尽的描述。③舆情分类。按照突发事件、敏感事件、社会、民生、政务等舆情组织的分类标准记录舆情

分类。④触发阈值。设置触发阈值,调用触发器开始或终止舆情应对。⑤舆情状态。记录舆情潜伏、爆发、消退、消亡等舆情演进状态。⑥风险等级。按照舆情风险管理组织设定的舆情风险"极高风险、高风险、一般风险、低风险、无风险"记录舆情等级。⑦舆情爆发概率。基于舆情分析模型对舆情爆发概率进行记录。⑧舆情影响力。根据舆情分析模型对舆情的影响力数值进行记录。如果一个舆情风险事件真实发生,还将记录对舆情应对目标的影响。⑨舆情应对计划。从正面回应、核查处理、一次回应、动态回应、动态监测、信息研判、责任切割、公信力修复等维度制定舆情应对计划。⑩舆情风险管理组织。对舆情风险管理基层组织、高层管理人员、新闻发言人、相关利益群体进行记录。

### 4.2.2 基于区块链的舆情风险关联树

完整的舆情风险登记表包括舆情风险分析分类账、舆情风险应对分类账和舆情风险汇总分类账,而基于区块链默克尔树构建的舆情风险关联树,通过分类帐建立对应关系,能够快速、低成本、自由地定位检索有关舆情风险登记账的最新信息,笔者构建的舆情风险关联树如图 4 所示。其中,事务树用于保存特定区块交易,收据树用于保存多个交易的详细数据,舆情风险关联树保存 3 种分类帐的包含关系。其中,前两棵树用于保障数据一致性并降低用户端的数据存储量级,从而克服传统舆情数据管理的缺陷。

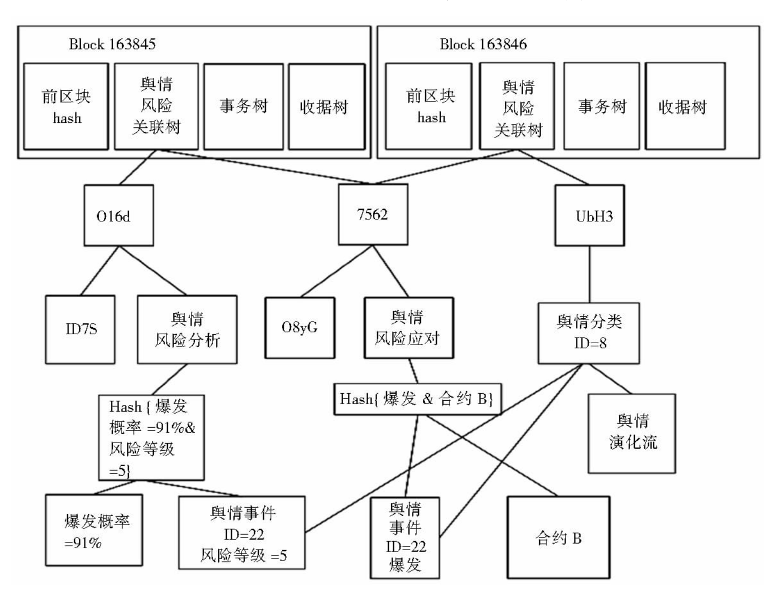



图 4 基于区块链的舆情风险关联树

舆情风险关联树建立了 3 种分类账之间的关联关系,通过散列关系能快速地相互关联。在图 4 中,块 163 845写入舆情风险分析分类账和舆情风险应对分类账,舆情风险综合分类账写入 163 846 号区块。舆情风险事件、舆情风险分析和舆情风险应对基于风险 hash 值进行响应。舆情风险事件 22 通过树节点关系得到舆情风险等级为 5、舆情风险为爆发的状态数据。在此过程中,每个区块链代理只需要下载相应的块头即可。例如,基于 163 846 区块中舆情事件 22 综合分类帐,可获取其舆情分析 ID 和舆情应对 ID 的对应 hash 值,进而在 163 845区块快速查找获取舆情事件 22 舆情风险分析和舆情风险应对数据。同样,如果已知舆情风险分析分类帐中对应舆情风险 ID,则可从 163 845 区块基于 hash 值定位 163 846 区块上的综合分类帐。

### 4.2.3 基于区块链的舆情风险智能合约

区块链数据保障系统共有 3 个智能合约:①智能合约 1。主要负责舆情控制关键绩效指标和关键绩效指标自动计算;获取舆情风险事件 ID 和类型;获取舆情风险事件交易分类帐、风险分析分类帐、风险应对台账;获取相应舆情风险汇总分类帐;基于舆情风险交易分类帐获取舆情事件 ID;生成汇总项目分类帐事务块并上链等待共识确认。②智能合约 2。负责舆情风险应对的级别审批和动态调整;获取舆情风险事件 ID 和类型;获取相应舆情风险交易分类账、应对分类账及风险应对台账;从舆情风险交易帐获取舆情事件 ID 以及汇总风险分类帐;计算舆情风险应对值;基于舆情影响力确定舆情应对级别规则;舆情风险状态发生变化的舆情事件,则生成新的舆情风险汇总分类帐中止舆情应对并呼叫智能合约 3 以达成共识;获取相应的舆情风险应对分类账建立汇总风险项分类帐;在风险应对分类账中基于舆情事件 ID 建立风险集合;根据变更后的舆情风险审批级别形成系统的响应计划;更新汇总分类帐中的审批级别并

提交共识。③智能合约3。负责舆情风险事件状态变更确认;获取相应舆情风险事件ID;基于区块链交易分类账确定舆情风险分析分类账或舆情风险应对台账中的舆情风险状态变化;基于区块链交易分类账获取相应的舆情风险汇总项最新舆情事件的ID;判断是否需要批准修改舆情风险识别、应对和报告状态。如果不允许修改状态,则生成挂起状态和新的汇总风险达成一致。如果允许修改状态,则上链等待共识确认。

## 5 研究结论

笔者基于网络舆情风险管理、弹性管理理论,确立了网络舆情弹性风险管理理论框架,进而应用区块链技术提出了网络舆情风险管理系统体系,并对网络舆情风险识别和感知智慧分类账本、风险关联树以及智能合约进行了阐述。

本研究在理论和实践层面均具有一定创新性。在理论层面,将网络舆情风险管理理论、弹性管理理论相结合,提出网络舆情弹性风险管理理论框架,深化了风险管理理论在网络舆情管理领域的应用。在网络舆情风险管理系统体系构建过程中,设计了网络舆情风险管理子系统和区块链数据保障子系统,并对网络舆情风险识别和感知智慧分类账本、风险关联树以及智能合约等区块链应用核心技术展开了详尽描述。弹性管理理论和网络舆情风险管理理论的价值在区块链技术的支撑下得以进一步深入挖掘。在实践层面,网络舆情风险管理理论框架具备的“管理弹性”可有效应对网络舆情均衡事件的高可变性和自适应性,区块链技术的应用则突破了传统风险管理系统的瓶颈,从而在网络舆情风险管理的全生命周期过程中,舆情风险管理数据更安全、数据可追溯、组织弹性适应性强、风险管理效率更高,能有效指引有关舆情风险管理部门基于区块链技术开发网络舆情风险管理系统,增强网络舆情风险管理可控性、提高网络舆情风险管理效率。

在研究过程中,因重点应用区块链技术解决网络舆情风险管理的核心问题,以及受篇幅限制,导致所构建管理体系中,未能对弹性风险管理架构进行更深入的设计。在后续研究中,将进一步展开弹性风险管理架构设计,并应用区块链技术开发网络舆情风险管理系统,重点解决如何协调线上线下舆情信息互动和交织问题,以典型舆情风险管理事件为实例说明所构建体系的科学性、先进性和可操作性。



**参考文献:**

[1] LEE B H, LEE J H. Blockchain-based secure firmware update for embedded devices in an Internet of things environment[J]. Journal of supercomputing,2017,73(3):1152－1167.
[2] CHAKRAVORTY A, RONG C. Ushare: user controlled social media based on blockchain[EB/OL]. [2019－09－27]. https://www.researchgate.net/publication/312211808_Ushare_user_controlled_social_media_based_on_blockchain.
[3] BUCHANAN N H. Social security is fair to all generations: demystifying the trust fund, solvency, and the promise to younger Americans[J]. Cornell journal of law & public policy, 2017, 27(2): 237.
[4] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11):15－17.
[5] TAPSCOTT D, TAPSCOTT A. How blockchain will change organizations[J]. MIT sloan management review, 2017,58(2):10－13.
[6] DORRI A, STEGER M, KANHERE S S, et al. BlockChain: a distributed solution to automotive security and privacy[J]. IEEE communications magazine, 2017, 55(12):119－125.
[7] KIM H W, JEONG Y S. Secure authentication-management human-centric scheme for trusting personal resource information on mobile cloud computing with blockchain[J]. Human-centric computing and information sciences,2018,8(1):11－20.
[8] GREINER M E, WANG H. Trust-free systems-a new research and design direction to handle trust-issues in P2P Systems[C]//21st Americas conference on information systems, AMCIS 2015. San Francisco:Curran Associates Inc, 2015:1－16.
[9] DMITRY E, PAVEL R. The All-Pervasiveness of the blockchain technology[J]. Procedia computer science,2018,123(1):116－121.
[10] BECK R, CZEPLUCH J S, LOLLIKE N, et al. Blockchain-the gateway to trust-free cryptographic transactions[EB/OL]. [2019－09－27]. https://www.researchgate.net/publication/302589859_BLOCKCHAIN_-_THE_GATEWAY_TO_TRUST-FREE_CRYPTOGRAPHIC_TRANSACTIONS.
[11] LUSTIG C, NARDI B. Algorithmic authority: the case of Bitcoin[C]//2015 48th Hawaii international conference on system sciences. New York: IEEE, 2015: 743－752.
[12] 李华强,范春梅,贾建民,等. 突发性灾害中的公众风险感知与应急管理——以5·12汶川地震为例[J]. 管理世界,2009(6):52－60,187－188.
[13] 王炼,贾建民. 突发性灾害事件风险感知的动态特征——来自网络搜索的证据[J]. 管理评论,2014,26(5):169－176.
[14] SUGIMOTO A, NOMURA S, TSUBOKURA M, et al. The relationship between media consumption and health-related anxieties after the Fukushima Daiichi nuclear disaster[J]. PLOS ONE, 2013, 8(8):e65331.
[15] 张玉亮. 基于发生周期的突发事件网络舆情风险评价指标体系[J]. 情报科学,2012,30(7):1034－1037,1043.
[16] 曾润喜,罗俊杰,朱美玲. 网络社会安全风险评估指标体系研究

[J]. 电子政务,2019(3):36 - 45.
[17] 马宁,刘怡君,廉莹. 突发事件舆情风险研究文献综述[J]. 情报杂志,2019,38(6):88 - 94.
[18] 王文艳,刘珍,王秋菊. 微博舆情风险识别与防范措施——以"3·1昆明暴恐事件"为例[J]. 新闻世界,2014(8):179 - 180.
[19] 陈培友,侯甜甜. 基于 ANP - 灰色模糊的社交网络舆情风险预警研究——以"重庆公交坠江事件"为例[J]. 情报科学,2019,37(5):115 - 120.
[20] YU L, LING L, LING T. What can mass media do to control public panic in accidents of hazardous chemical leakage into rivers? a multi-agent-based online opinion dissemination model[J]. Journal of cleaner production, 2017, 143(1):1203 - 1214.
[21] 曾润喜,陈创. 基于非传统安全视角的网络舆情演化机理与智慧治理方略[J]. 现代情报,2018,38(11):9 - 13.
[22] ARQUAM M, SINGH A, SHARMA R. A blockchain based secure and trusted framework for information propagation on online social networks[J]. Computer science,2018, 62(4):1157 - 1164.
[23] MA S, HAO W, DAI H N, et al. A blockchain-based risk and information system control framework[C]// 2018 IEEE 16th intl conf on dependable, autonomic and secure computing, 16th intl conf on pervasive intelligence and computing, 4th intl conf on big data intelligence and computing and cyber science and technology congress (DASC/PiCom/DataCom/CyberSciTech). New York: IEEE, 2018: 106 - 113.
[24] HUANG H D, HONG P W, LEE Y T, et al. SOC: hunting the underground inside story of the ethereum Social-network Opinion and Comment[J]. Computer science,2018, 62(3):156 - 161.
[25] 赵丹,王晰巍,韩洁平,等. 区块链环境下的网络舆情信息传播特征及规律研究[J]. 情报杂志,2018,37(9):127 - 133,105.
[26] 宾晟,孙更新,周双. 基于区块链技术的社交网络中舆情传播模型[J]. 应用科学学报,2019,37(2):191 - 202.
[27] 黄心豪,赵博. 基于区块链技术的网络舆论优化研究[J]. 中国传媒科技,2019(1):48 - 51.
[28] 陈鹤杰,闫强. 基于大数据技术的热点事件图书舆情研究[J]. 科技与出版,2019(4):83 - 85.
[29] 丁晓蔚,高淑萍. 虚拟货币:金融及舆情风险管理探讨[J]. 现代传播(中国传媒大学学报),2018,40(1):133 - 139.
[30] 李泰安. 区块链重构网络舆论环境[J]. 传媒,2017(21):87 - 90.
[31] DEMEK K C, RASCHKE R L, JANVRIN D J, et al. Do organizations use a formalized risk management process to address social media risk? [J]. International journal of accounting information systems, 2017(28):31 - 44.
[32] 吕文栋,王晓飞,赵杨. 基于组织弹性视角再议风险管理[J]. 管理现代化,2017,37(4):101 - 104.

**作者贡献说明：**

郭苏琳：论文撰写及最终版本修订,数据处理及实证研究；

黄微：提出研究命题及研究思路；

李吉：论文修改。



## Research on the Application of Block Chain Technology in Network Public Opinion Risk Management System

Guo Sulin　Huang Wei　Li Ji
School of Management, Jilin University, Changchun 130022

Abstract: [**Purpose/significance**] To explore the application value of flexible management and block chain theory in the construction of network public opinion risk management system, overcome the technical drawbacks of traditional management system, directly hit the existing difficulties and pain points of network public opinion risk management, and improve the efficiency of network public opinion risk management. [**Method/process**] Based on the theory of risk management and elasticity management of network public opinion, this paper established the theoretical framework of elasticity risk management of network public opinion, and then proposed a risk management system of network public opinion by using block chain technology. It elaborated on risk identification ledger, risk association tree and intelligent contract in detail. [**Result/conclusion**] This paper constructs the public opinion risk management system and block chain data guarantee system. Based on block chain technology, it designs perceptual intelligence ledger, risk association tree and intelligent contract. It makes public opinion risk management data safer, data traceable and more adaptable to organizational flexibility. This study can effectively guide the development of relevant systems, enhance the controllability of network public opinion risk management, and improve the efficiency of network public opinion risk management.

Keywords: block chain　network public opinion　risk management